

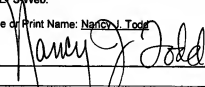
**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

Applicants:	Luis Barriga Caceres, <i>et al.</i>	§	Group Art Unit:	2437
Application No	10/595,025	§	Examiner:	Pham, Luu T.
Filed:	12/21/2005	§	Confirmation No:	1351
Attorney Docket No:	P18155-US1	§		
Customer No.:	27045	§		

For: Apparatus and Method for a Single Sign-On Authentication Through a Non-Trusted Access Network

**Via EFS-Web**

Mail Stop Appeal Brief - Patents  
Commissioner for Patents  
P. O. Box 1450  
Alexandria, VA 22313.1450

<p align="center"><b><u>CERTIFICATE OF TRANSMISSION BY EFS-WEB</u></b></p> <p>Date of Transmission: August 18, 2009</p> <p>I hereby certify that this paper or fee is being transmitted to the United States Patent and Trademark Office electronically via EFS-Web.</p> <p>Type or Print Name: <u>Nancy J. Todd</u></p> <p></p>
---

**APPEAL UNDER 35 U.S.C. §134**

This Brief is submitted in connection with the decision of the Primary Examiner set forth in Final Official Action dated February 18, 2009 and Advisory Action dated April 27, 2009, finally rejecting claims 24-27 and 29-46, which are all of the pending claims in this application.

The Commissioner is hereby authorized to charge any appropriate fees under 37 C.F.R. §41.20(b)(2) that may be required by this paper, and to credit any overpayment, to Deposit Account No. 50-1379.

**Real Party in Interest**

The real party in interest, by assignment, is: Telefonaktiebolaget LM Ericsson (publ)  
SE-164 83  
Stockholm, Sweden

### **Related Appeals and Interferences**

None.

### **Status of Claims**

Claims 1-23, 28 were previously cancelled and are not appealed. Claims 24-27 and 29-46 are pending in the present application, each of which are finally rejected and form the basis for this Appeal. Claims 24-27 and 29-40 stand rejected, under 35 U.S.C. §101/§112 on the asserted basis that those claims are directed to "non-statutory subject matter and found indefinite." Claims 24-27, 29-30, 37, and 41-45 stand rejected, under 35 U.S.C. §103(a) as being unpatentable over Jin, *et al.* (U.S. Patent No. 6,643,782) in view of Montenegro (U.S. Patent No. 6,571,289); and claims 31-36, 38-40 and 46 as being unpatentable over Jin in view of Montenegro and Schneider, *et al.* (U.S. Patent No. 6,105,027). Claims 24-27 and 29-46, including all amendments to the claims, are attached in the Claims Appendix. The rejection of claims 24-27 and 29-46 is appealed.

### **Status of Amendments**

The claims set out in the Claims Appendix include all entered amendments. No amendment has been filed subsequent to the final rejection.

### **Summary of Claimed Subject Matter**

<b>Claim Element</b>	<b>Specification Reference</b>
24. An apparatus arranged for receiving a Single Sign-On service request in a telecommunication service network from a user via an access network unable to provide data origin authentication, the user having received access credentials as a result of being authenticated by a core network, the apparatus comprising:	Figures 2 and 3 Paragraphs [0049], [0050], [0052] and [0058]
means for receiving, at a Secure Service Entry Point of the service network, the access credentials from the user through the access network;	Paragraph [0059]
means for checking at the Secure	Paragraphs [0059] and [0060]

<b>Claim Element</b>	<b>Specification Reference</b>
Service Entry Point validity of the access credentials received from the user;	
means for establishing a valid session with the user from the Secure Service Entry Point upon successful validity check of the access credentials;	Paragraphs [0059] and [0060]
means for assigning an internal IP address between the Secure Service Entry Point and a Single Sign-On server to identify the user in the service network;	Paragraph [0061] last sentence
means for linking at the Single Sign-On server session data, access credentials and assigned internal IP address for the user; and,	Paragraph [0062]
means for establishing a secure tunnel with the user from the Secure Service Entry Point when receiving the access credentials through the access network by using an outer IP address assigned to the user by the access network for addressing the user, and by using the internal IP address assigned to identify the user in the service network as an inner IP address in the tunnelled traffic.	Paragraphs [0010], [0014], [0018], [0043], [0044], [0051] and [0061]

<b>Claim Element</b>	<b>Specification Reference</b>
37. A user equipment arranged to carry out an authentication procedure with a core network, and arranged to access a telecommunication service network via an access network unable to provide data origin authentication, the user equipment, comprising:	Paragraphs [0042] and [0043]
means for obtaining access credentials from an Authentication Server of the core network as a result of being authenticated by the core network;	Paragraphs [0044] and [0050]
means for sending the access credentials towards a Secure Service Entry Point of the service network when accessing through the access network;	Paragraph [0059]
means for establishing a secure tunnel with the Secure Service Entry Point of the service network through the access network,	Paragraph [0025], [0059] and [0060]

<b>Claim Element</b>	<b>Specification Reference</b>
the secure tunnel making use of an outer IP address assigned to the user by the access network for addressing the user;	
means for receiving an internal IP address assigned by the service network and included as an inner IP address within the tunnelled traffic to identify the user in the service network; and,	Paragraph [0062]
means for linking said access credentials with the inner IP address and with the secure tunnel.	Paragraph [0062]

<b>Claim Element</b>	<b>Specification Reference</b>
41. A method for supporting Single Sign-On services in a telecommunication service network for a user accessing said service network through an access network unable to provide data origin authentication, the user having received access credentials as a result of being authenticated by a core network, the method comprising the steps of:	Paragraph [0029], [0042] and [0043]
receiving at the service network the access credentials from the user through the access network;	Paragraph [0059]
checking validity of the access credentials received at the service network;	Paragraphs [0059] and [0060]
establishing a valid session with the user upon successful validity check of the access credentials;	Paragraphs [0059] and [0060]
assigning at the service network an internal IP address for the user to identify the user when accessing a service in the service network;	Paragraph [0061]
linking session data, access credentials and the assigned internal IP address for the user at an entity of the service network;	Paragraph [0062]
establishing a secure tunnel between the user equipment side and an entity of the service network through the access network by using an outer IP address assigned by the access network for addressing the user, and by using as an inner IP address in the	Paragraphs [0010], [0014], [0018], [0043], [0044], [0051] and [0061]

Claim Element	Specification Reference
tunnelled traffic the internal IP address assigned to identify the user in the service network; and,	
linking said access credentials with said inner IP address and with said secure tunnel at the user equipment side.	Paragraph [0062]

In addition to those referenced portions of the specification, it is important to note that those skilled in the art understand that an IP packet consists of, firstly, an address overhead portion with originating and destination addresses for addressing both ends of the communication and, secondly, a packet payload portion. In accordance with the Applicants' invention and with the prior art discussed at paragraphs [0010] and [0014], an outer IP address is assigned to the user by the access network for addressing the user, and thus being allocated as part of the address overhead portion as known to those skilled in the art. Since the access network is not trustable, however, the outer IP address can be used by an attacker performing IP spoofing. To overcome this drawback, the Applicants' invention provides for the additional provision of an internal IP address, assigned by the service network to identify the user therein, and which is included as an inner IP address in the tunnelled traffic; *i.e.*, in the packet payload portion. In other words, two IP addresses are assigned to the same entity, namely, to the user equipment, and both are used within the secure tunnel: an outer IP address assigned by the access network for addressing purposes, and thus included in the address overhead portion and, according to the principles of the invention, an inner IP address assigned by the service network to securely identify the user, and thus included as payload in the tunnelled traffic and not being part of the address overhead portion. Both the outer IP address assigned by the access network and the inner IP address assigned by the service network are necessarily two different IP addresses (as assigned by different networks with different network masks, *etc.*) corresponding to the same entity (namely, the user) accompanying the packet (the outer IP address as part of the packet header and the inner IP address included in the packet payload) and are used for different purposes; *i.e.*, the outer IP address is used for addressing the user,

whereas the inner IP address is used for identification of the user in the service network to preclude IP-address spoofing.

The specification references listed above are provided solely to comply with the USPTO's current regulations regarding appeal briefs. The use of such references should not be interpreted to limit the scope of the claims to such references, nor to limit the scope of the claimed invention in any manner.

### **Grounds of Rejection to be Reviewed on Appeal**

- 1.) Whether claims 24-27 and 29-40, rejected under 35 U.S.C. §101/§112, are directed to statutory subject matter and are definite;
- 2.) Whether claims 24-27, 29-30, 37, and 41-45, rejected under 35 U.S.C. §103(a), are patentable over Jin, *et al.* (U.S. Patent No. 6,643,782) in view of Montenegro (U.S. Patent No. 6,571,289); and,
- 3.) Whether claims 31-36, 38-40 and 46, rejected under 35 U.S.C. §103(a), are patentable over Jin in view of Montenegro and Schneider, *et al.* (U.S. Patent No. 6,105,027).

### **Arguments**

#### **1.) Rejection of Claims 24-27 and 29-40 under 35 U.S.C. §101 / §112**

The Examiner has rejected claims 24-27, and 29-40 on the asserted basis that those claims are directed to "non-statutory subject matter and found indefinite." The Applicants traverse the rejections.

In the office action dated July 9, 2008, the Examiner rejected the claims under §101 on the asserted basis that the claims recite "means for" claims limitations without "integrating a machine (e.g., a computer)." In addition, the Examiner rejected the claims under §112 on the asserted basis that they recite "means for" claim elements with no structure disclosed in the specification. In response, the Applicants noted that the functions performed by the various "means for" elements, as authorized under §112, Paragraph 6, are disclosed as being performed by conventional telecommunications network elements known to those skilled in the art as various general or specific-purpose computers. In maintaining the rejections under §§101 and 112, the Examiner is

conflating the principles enunciated by the Federal Circuit and U.S. Supreme Court in the cases of *Cominsky* (499 F.3d 1365, Fed. Cir. 2007), *Bilski* (88 USPQ2d 1385) and *Biomedino* (490 F.3d 946, Fed. Cir. 2007).

First, claims 24-27 and 29-40 are directed to statutory subject matter. Each of those claims is directed to an apparatus wherein certain “means for” performing each of a novel combination of functions are performed. Not only do the claim preambles limit the claims to an apparatus, but such “means for” elements are statutorily authorized under §112, ¶6: “An element in a claim for a combination may be expressed as a means . . . for performing a specified function without the recital of structure . . . , and such claim shall be construed to cover the corresponding structure . . . described in the specification and equivalents thereof.” (emphasis added) The functions recited in those claims are identified in the specification as being performed by various network nodes, including a “Secure Service Entry Point” and a “Single Sign-On server,” which are, in fact, explicitly recited in the claims. Neither *In re Cominsky* or *In re Bilski* were concerned with the question of whether claims drafted in accordance with §112, ¶6, qualified as statutory subject matter. In fact, it would be incongruous to the patent statute, as a whole, to state that claims can be drafted using the statutorily-authorized form under §112, ¶6, yet not qualify as statutory subject matter under §101.

The foregoing is also supported by the Federal Circuit’s opinion in *Biomedino*, in which the court stated that:

Once a court concludes that a claim limitation is a means-plus-function limitation, two steps of claim construction remain: 1) the court must first identify the function of the limitation; and 2) the court must then look to the specification and identify the corresponding structure for that function. If there is no structure in the specification corresponding to the means-plus function limitation in the claims, the claim will be found invalid as indefinite. While the specification must contain structure linked to claimed means, this is not a high bar. “[a]ll one needs to do in order to obtain the benefit of [§ 112, ¶ 6] is to recite **some** structure corresponding to the means in the specification, as the statute states, so that one can readily ascertain what the claim means and comply with the particularity requirement of [§ 112,] ¶ 2.” Additionally, interpretation of what is disclosed in the specification must be made in light of the knowledge of one skilled in the art. Thus, in order for a means-plus-function claim to be valid under § 112, the corresponding structure of the limitation “must be disclosed in the written description in such a manner that one skilled in the art will know

and understand what structure corresponds to the means limitation. Otherwise, one does not know what the claim means." (emphasis added)

One of ordinary skill in the art would readily ascertain, from a reading of Applicants' specification, the means necessary to carry out the recited claim functions using the telecommunications nodes and elements clearly depicted in the figures and described with reference thereto. Accordingly, claims 24-27, and 29-40 satisfy the requirements of §§101 and 112.

**2.) Rejection of claims 24-27, 29-30, 37, and 41-45, under 35 U.S.C. §103(a)**

The Examiner rejected claims 24-27, 29-30, 37, and 41-45 as being unpatentable over Jin, *et al.* (U.S. Patent No. 6,643,782) in view of Montenegro (U.S. Patent No. 6,571,289). The Applicants traverse the rejections.

In the Final Office Action (FOA) dated February 18, 2009, the Examiner did not provide any substantive response to the arguments present by Applicants in response to the prior office action. The Examiner again acknowledged that Jin does not disclose establishing a secure tunnel by using an outer IP address assigned to the user by the access network for addressing the user, and by using the internal IP address assigned to identify the user in the service network as an inner IP address in the tunneled traffic. (FOA; page 12, line 1, *et seq.*) To overcome that deficiency, the Examiner has looked to the teachings of Montenegro.

Montenegro discloses a plurality of tunnel segments composing a chain of a registration request from a mobile node to a private network. More particularly, Montenegro discloses (see: column 4, lines 14-36) that when a correspondent node, whose address is CN, desires to send a packet of information to a mobile node, whose address is MN, in a private network, the correspondent node will compose a packet with a source address of CN and a destination address of MN. This packet is intercepted by a Home Agent in the private network, whose address is HA, and the Home Agent forwards such packet to a Gateway, whose address is GW, by pre-pending an additional header with a source address of HA and a destination address of GW. The Gateway receives such packet and strips off the added header to recover the original packet with source address of CN and destination address of MN, and encounters that



such MN address has a binding in the GW with an address of a Foreign Agent, whose address is FA. This binding makes the Gateway prepend (*i.e.*, prefix) its own new header with source address of GW and destination address of FA. The Foreign Agent receiving such packet also strips off the latest header and recovers the original packet with source address of CN and destination address of MN. From this teaching in Montenegro, it can be seen that the original packet has a unique header with a source address of CN and a destination address of MN when submitted between the correspondent node and the Home Agent as well as when submitted between the Foreign Agent and the mobile node in the private network; and the original packet has an additional header prepended to the original packet, with source address of HA and a destination address of GW, when submitted between the Home Agent and the Gateway, and another additional header pre-pended to the original packet, with source address of GW and a destination address of FA, when submitted between the Gateway and the Foreign Agent. In other words, Montenegro discloses more than one source address and more than one destination address for a same unique packet, wherein the more than one source address and wherein the more than one destination address always correspond to **different** entities.

Montenegro thus fails to anticipate two different IP addresses corresponding to the **same** entity accompanying the packet and used for different purposes. More specifically, Montenegro fails to disclose an *outer* IP address assigned to the user by the access network for addressing the user and an *internal* IP address assigned to identify the user in the service network as an inner IP address in the tunneled traffic. Therefore, even if disclosing secure tunnels, Montenegro fails to teach means for establishing a secure tunnel with a user from a Secure Service Entry Point when receiving access credentials through an access network **by using an outer IP address assigned to the user by the access network for addressing the user, and by using the internal IP address assigned to identify the user in the service network as an inner IP address in the tunneled traffic.** Accordingly, claim 24 is not obvious over Jin in view of Montenegro. Similarly, whereas claims 37 and 41 recite analogous limitations, they are also not obvious in view of those references. Furthermore, whereas claims 25-27, 29 and 30 are dependent from claim 24, and claims 42-44 are dependent from claim

41, and include the limitations of their respective base claims, they are also not obvious in view of those references.

**3.) Rejection of claims 31-36, 38-40 and 46 under 35 U.S.C. §103(a)**

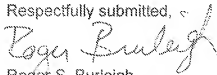
The Examiner rejected claims 31-36, 38-40 and 46 as being unpatentable over Jin in view of Montenegro and Schneider, *et al.* (U.S. Patent No. 6,105,027). The Applicants traverse the rejections.

As established *supra*, independent claims 24, 37 and 41 are not obvious over Jin in view of Montenegro. The Examiner has not pointed to any teaching in Schneider to overcome the deficiencies in those references. Accordingly, whereas claims 31-36, 38-40 and 46 are dependent from claims 24, 37 and 41, respectively, and include the limitations of their base claim, the Examiner has not established a *prima facie* case of obviousness in view of Jin, Montenegro and Schneider.

\* \* \*

CONCLUSION

The claims currently pending in the application are patentable over the cited references and the Applicants request that the Examiner's claim rejections be reversed and the application be remanded for further prosecution.

Respectfully submitted, 

Roger S. Burleigh  
Registration No. 40,542  
Ericsson Patent Counsel

Date: August 18, 2009

Ericsson Inc.  
6300 Legacy Drive, M/S EVR1 C-11  
Plano, Texas 75024

(972) 583-5799  
roger.burleigh@ericsson.com

## **CLAIMS APPENDIX**

1-23. (Cancelled)

24. (Previously Presented) An apparatus arranged for receiving a Single Sign-On service request in a telecommunication service network from a user via an access network unable to provide data origin authentication, the user having received access credentials as a result of being authenticated by a core network, the apparatus comprising:

means for receiving, at a Secure Service Entry Point of the service network, the access credentials from the user through the access network;

means for checking at the Secure Service Entry Point validity of the access credentials received from the user;

means for establishing a valid session with the user from the Secure Service Entry Point upon successful validity check of the access credentials;

means for assigning an internal IP address between the Secure Service Entry Point and a Single Sign-On server to identify the user in the service network;

means for linking at the Single Sign-On server session data, access credentials and assigned internal IP address for the user; and,

means for establishing a secure tunnel with the user from the Secure Service Entry Point when receiving the access credentials through the access network by using an outer IP address assigned to the user by the access network for addressing the user, and by using the internal IP address assigned to identify the user in the service network as an inner IP address in the tunnelled traffic.

25. (Previously Presented) The apparatus of claim 24, wherein the Single Sign-On Server comprises means for generating service credentials for authorizing the user to access a service in the service network.

26. (Previously Presented) The apparatus of claim 25, wherein the service credentials are generated on a per service basis for the user upon service request.

27. (Previously Presented) The apparatus of claim 24, wherein the Secure Service Entry Point comprises means for communicating with an Authentication Server of the home network in order to check the validity of the access credentials received from the user when said access credentials are not signed by a recognised authentication entity.

28. (Cancelled).

29. (Currently Amended) The apparatus of claim ~~28~~ 24, further comprising means for communicating the Secure Service Entry Point with the Single Sign-On Server.

30. (Previously Presented) The apparatus of claim 24, wherein the Single Sign-On Server comprises means for an additional co-ordination between the apparatus and an Identity Provider in charge of said user in a home network when said home network is different than the service network which the apparatus is the entry point for.

31. (Previously Presented) The apparatus of claim 24 for use when the user is accessing a local HTTP service, or an external service in a network different than the currently accessed service network, wherein the Single Sign-On Server comprises means for checking whether the user had been previously authenticated or not.

32. (Previously Presented) The apparatus of claim 31, wherein the Secure Service Entry Point comprises means for communicating with an intermediate entity arranged to intercept the user's access to the HTTP local service, or to the external service in an external network.

33. (Previously Presented) The apparatus of claim 32, wherein the intermediate entity is an HTTP-proxy.

34. (Previously Presented) The apparatus of claim 32, wherein the intermediate entity is a firewall.

35. (Previously Presented) The apparatus of claim 24 for use when the user is accessing a non-HTTP local service, wherein the Single Sign-On Server comprises means for checking whether the user had been previously authenticated or not.

36. (Previously Presented) The apparatus of claim 24, wherein the means for receiving access credentials at the Secure Service Entry Point comprises means for checking whether a digital certificate issued by the core network is present to indicate a successful authentication of the user.

37. (Previously Presented) A user equipment arranged to carry out an authentication procedure with a core network, and arranged to access a telecommunication service network via an access network unable to provide data origin authentication, the user equipment, comprising:

- means for obtaining access credentials from an Authentication Server of the core network as a result of being authenticated by the core network;

- means for sending the access credentials towards a Secure Service Entry Point of the service network when accessing through the access network;

- means for establishing a secure tunnel with the Secure Service Entry Point of the service network through the access network, the secure tunnel making use of an outer IP address assigned to the user by the access network for addressing the user;

- means for receiving an internal IP address assigned by the service network and included as an inner IP address within the tunnelled traffic to identify the user in the service network; and,

- means for linking said access credentials with the inner IP address and with the secure tunnel.

38. (Previously Presented) The user equipment of claim 37, wherein the means for obtaining access credentials includes:

means for receiving an authentication challenge from the Authentication Server of the core network;

means for generating and returning an authentication response to the Authentication Server of the core network;

means for generating a public and private key pair; and,

means for submitting the public key along with a digital signature proving the ownership of the private key towards the Authentication Server of the core network.

39. (Previously Presented) The user equipment of claim 37, wherein the means for obtaining access credentials includes:

means for receiving an authentication challenge from the Authentication Server of the core network;

means for generating and returning an authentication response to the Authentication Server of the core network; and,

means for requesting a digital certificate obtainable from the core network.

40. (Previously Presented) The user equipment of claim 39, wherein the means for obtaining access credentials further includes means for generating a public key for which the digital certificate is obtainable.

41. (Previously Presented) A method for supporting Single Sign-On services in a telecommunication service network for a user accessing said service network through an access network unable to provide data origin authentication, the user having received access credentials as a result of being authenticated by a core network, the method comprising the steps of:

receiving at the service network the access credentials from the user through the access network;

checking validity of the access credentials received at the service network;

establishing a valid session with the user upon successful validity check of the access credentials;

assigning at the service network an internal IP address for the user to identify the user when accessing a service in the service network;

linking session data, access credentials and the assigned internal IP address for the user at an entity of the service network;

establishing a secure tunnel between the user equipment side and an entity of the service network through the access network by using an outer IP address assigned by the access network for addressing the user, and by using as an inner IP address in the tunnelled traffic the internal IP address assigned to identify the user in the service network; and,

linking said access credentials with said inner IP address and with said secure tunnel at the user equipment side.

42. (Previously Presented) The method of claim 41, further comprising a step of generating service credentials for authorizing the user to access a service in the service network.

43. (Previously Presented) The method of claim 42, wherein the step of generating service credentials includes a step of generating service credentials on a per service basis for the user upon service request.

44. (Previously Presented) The method of claim 41, wherein the step of checking the validity of access credentials received from the user at the service network further includes a step of communicating with an Authentication Server of the home network when said access credentials are not signed by a recognised authentication entity.

45. (Previously Presented) The method of claim 41, wherein the step of linking session data, access credentials and assigned internal IP address for the user further includes a step of communicating a first device named Secure Service Entry Point in charge of the secure tunnel with a second device named Single Sign On Server where the step of linking takes places.



46. (Previously Presented) The method of claim 41, for use when the user is accessing a local service or an external service in a network different than the currently accessed service network, the method further comprising a step of checking whether the user had been previously authenticated or not.

\* \* \*

**EVIDENCE APPENDIX**

None.

**RELATED PROCEEDINGS APPENDIX**

None.